AB:AXB

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE BASEMENT, THE FIRST FLOOR, AND SO MUCH OF THE SECOND FLOOR OF THE PREMISES KNOWN AS 590 EDGEGROVE AVENUE, STATEN ISLAND, NEW YORK 10312, AS IS OCCUPIED BY KAREN DIAMOND	**TO BE FILED UNDER SEAL** **APPLICATION FOR A SEARCH WARRANT FOR A PREMISES AND ELECTRONIC DEVICES FOUND THEREIN** No. 18 MJ 938

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, AMANDA YOUNG, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the basement, the first floor, and so much of the second floor of the premises known as 590 Edgegrove Avenue, Staten Island, New York 10312 (collectively, the "PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since March 2017. Since October 2017, I have been assigned to a Crimes Against Children squad. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily

work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of multiple child pornography cases. Among other things, I have conducted or participated in surveillance, the execution of search warrants, and the review of electronic evidence, including reviewing thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

3. Based on the following paragraphs, I submit that there is probable cause to search the PREMISES for evidence of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

4. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

Bittorrent Peer to Peer File Sharing

6. Peer to Peer ("P2P") file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others who are running compatible P2P software. Bittorrent is one type of P2P software, which sets up its searches by keywords, typically on torrent websites. Bittorrent programs are typically free to download and are used to exchange files between computer users.

7. A user can use the software to perform a keyword search over the Internet. The results of a keyword search are displayed to the user via a website. The website itself does not contain the actual files intended to be shared, but instead provides a "torrent" file. A torrent is a small file that describes the files to be shared and provides details allowing the user to identify which of the available files he or she may wish to access. The user then selects which torrent file(s) from among the results to download. This torrent file contains download instructions for the user to download the file(s) referenced in the torrent that he/she wishes to access. The file can be downloaded through a direct connection between the computer requesting the file(s) and the computer(s) sharing the file(s). For example, a person interested in obtaining child pornography images could open the Bittorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search would then

be returned to the user's computer and displayed on the torrent site. The user then selects a torrent from among the results displayed corresponding to the file(s) he/she wants to download. Once the torrent file is downloaded, a previously-installed Bittorrent program is used to access the file content. The torrent file provides the set of instructions that the Bittorrent program needs to find the files identified in the torrent file. The file(s) are then downloaded directly from the sharing computer(s). The downloaded file(s) are stored in an area designated by the user and/or the software. The downloaded file(s) will remain in that location until moved or deleted.

8. P2P file sharing allows multiple files to be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Bittorrent user downloading an image file may actually receive parts of the image from multiple computers. This speeds up the time it takes to download the file.

9. A P2P file transfer is assisted by reference to an IP address. This address is unique to a particular computer or router during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

10. The computer running the file sharing application, in this case a Bittorrent application, has an IP address assigned to it while it is connected to the Internet. Bittorrent users are able to see the IP address of any computer system sharing files with or receiving files from them. When investigating subjects who share or access child pornography via P2P applications, investigators log the IP address that has sent them files or information regarding files being shared. Investigators can then search public records that are available on the Internet to

determine the Internet service provider who has been assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider.

The Investigation

11. On or about May 5, 2018, a FBI Special Agent working in an undercover capacity (the "Undercover Agent"), used a Bittorrent application via an Internet-connected computer located within the FBI New York Division to conduct undercover investigations into the Internet distribution and possession of child pornography. During this investigation, a computer that was sharing child pornography was located on the Bittorrent file sharing network. The Undercover Agent downloaded approximately 30 files associated with child pornography from IP address 100.33.35.174. The sharing client's IP address was recorded along with the date and time of the file transfer. The sharing client reported that it was using Bittorrent client software libtorrent, version 1.2.0.0. Your Affiant reviewed the files downloaded. Several of these files, which are available for the Court's review, are described as follows:

a. **Pthc 2013 4yo girl loves blowjob KITTY-VIP090** is an approximate 1 minute and 33 second video of an approximate 4 year old female being orally penetrated by an adult male penis.

b. **pthc PedolandFrifam RCA-4 5yr girl Only the Best** is an approximate 5 minute and 44 second video of an approximately 5 year old girl being digitally penetrated, orally penetrated by an adult male penis, and vaginally penetrated by an adult male penis.

c. **(kinderkutje) (Pthc)_FromVHS_8Yo Rape And Scream_!!!** is an approximately 53 minute video of an approximate 8 year old female being digitally penetrated in her vagina and anus, orally penetrated by an adult male penis, vaginally penetrated by an adult male tongue, and anally penetrated by an adult male penis.

d. **HMM – Melissa 7yrs set 5 - cum** is an approximate 2 minute and 31 second video of an approximate 7 year old being orally penetrated by an adult male penis.

12. The Bittorrent application used by the FBI captures the IP address from which the files were sent. All of the above files were downloaded from the IP address 100.33.35.174. Open source database searches revealed the IP address 100.33.35.174 was registered to Verizon Internet Services.

13. Based on a search of the IP Address in a law enforcement database, I learned that between June 19, 2017, and August 12, 2018, the IP Address regularly shared files known to be associated with child pornography and/or child erotica.

14. Records obtained from Verizon by administrative subpoena show that on May 5, 2018, Verizon had assigned the IP address 100.33.35.174 to "590 Edgegrove Avenue, Staten Island, New York 10312." The name of the subscriber to the Verizon account is Karen Diamond.

The Premises

15. The PREMISES is a multi-family home located on Edgegrove Avenue in Staten Island. The building is made of red brick, is two stories tall with a detached tan garage/storage shed and white balcony directly above the front door. The number 590 is directly to the right of the front door in white lettering. There is a side door to the left of the building and a fenced in back yard with the entrance to the fence near the side door.

16. The second story of the PREMISES is partitioned into two separate units. One of those units is believed to be occupied by Andrea Tanzillo. In this regard, a search of Con Edison records revealed that an open Con Edison account exists in the name of Andrea Tanzillo and

relates to one second-floor unit at the PREMISES. Furthermore, agents conducted a ruse at the PREMISES and spoke to Karen Diamond, who confirmed that she rents out a unit on the second floor of the PREMISES, which she believes utilizes an internet connection that is separate from the connection used in the remainder of the house.

17. The basement, the first floor, and the remaining second-floor unit are all believed to be occupied by Karen Diamond and her adult son. In this regard, a search of Con Edison records revealed that an open Con Edison account exists in the name of Karen Diamond and relates to the first floor of the PREMISES. During the conversation with agents described above, Karen Diamond confirmed that she owns the basement, the first floor, and the portion of the second floor of the PREMISES that is not occupied by Andrea Tanzillo.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computer: The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

b. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a

series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

NON-TECHNICAL TERMS

19. For the purposes of the requested warrant, the following non-technical terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8), in pertinent part, as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ."[1]

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

---

[1] See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. *Characteristics of Collectors of Child Pornography.* I further submit that, given the nature of the crimes under investigation, if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for the following additional reasons:

a. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

b. I know that collectors of child pornography typically retain their materials and related information for many years.

c. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

d. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are

known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

e. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

f. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs

may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the

owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to possess, access with intent to view, transport, receive, distribute or reproduce child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

26. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.[2]

27. Within 72 hours of the seizure of any computer devices, storage media, and related electronic equipment, law enforcement personnel will determine whether there exists articulable probable cause to believe that any of the seized items contain evidence, fruits, and instrumentalities of violations of the subject offenses. If law enforcement personnel determines that such articulable probable cause exists, the government will maintain possession of the seized items for the duration of any resulting investigation. If law enforcement cannot determine

---

[2] As a matter of practice, the FBI diligently reviews all electronic devices seized during a search warrant. If the device appears to belong to an innocent third party, the FBI releases the device as soon as the device has been imaged and has been confirmed to be "clean," i.e., does not contain any contraband or evidence of a crime. Until a given electronic device has been examined, there is no way to determine whether it was used to facilitate the criminal conduct under investigation or whether items relevant to the investigation have been transferred to such device.

whether such articulable probable cause exists, law enforcement personnel will return the seized items to the seized property owner within 72 hours or apply to the appropriate court within 72 hours for permission to retain the seized items for an additional period.

FORFEITURE

28. This application requests the issuance of a warrant under 21 U.S.C. § 853(f) authorizing the seizure of property subject to forfeiture. This is appropriate because: (1) there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, and (2) an order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture. There is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, because 18 U.S.C. § 2253(a) provides that the defendant's interest in: (1) "any visual depiction" proscribed by 18 U.S.C. §§ 2252 and 2252A, among others, or any book, magazine, periodical, film, videotape, or other matter which contains any such visual depiction, which was produced, transported, mailed, shipped or received in violation of" Chapter 18 of the United States Code; (2) "any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense"; and (3) "any property, real or personal, used or intended to be used to commit or to promote the commission of such offense or any property traceable to such property," shall be forfeited to the United States.

CONCLUSION

29. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as

they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Amanda Young
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on October 3, 2018

S/ Scanlon

Honorable Vera M. Scanlon
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 590 Edgegrove Avenue, Staten Island, New York (the "PREMISES"). The PREMISES is a multi-family home located on Edgegrove Avenue in Staten Island. The building is made of red brick, is two stories tall with a detached tan garage/storage shed and white balcony directly above the front door. The number 590 is directly to the right of the front door in white lettering. There is a side door to the left of the building and a fenced in back yard with the entrance to the fence near the side door.

This warrant authorizes searching the basement, the first floor, and so much of the second floor of the PREMISES as is occupied by Karen Diamond and/or her adult son. This warrant does not authorize a search of that portion of the PREMISES that is occupied exclusively by Andrea Tanzillo.

ATTACHMENT B

Property to be seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers[3] or storage media[4] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

---

[3] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

[4] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

16. Records and things evidencing the use of the Internet Protocol address 104.162.123.233, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.